Three dimensional quantum key distribution in the presence of several eavesdroppers

M. Daoud[a,b1] and **H. Ez-zahraouy**[c2]

[a] *Max Planck Institute for the Physics of Complex Systems Dresden, Germany*

[b] *Department of Physics, Faculty of Sciences, University Ibn Zohr, Agadir , Morocco*

[c] *LMPHE (URAC), Faculty of Sciences, University Mohammed V-Agdal, Rabat, Morocco*

Abstract

Quantum key distribution based on encoding in three dimensional systems in the presence of several eavesdroppers is proposed. This extends the BB84 protocol in the presence of many eavesdroppers where two-level quantum systems (qubits) are replaced by three-level systems (qutrits). We discuss the scenarios involving two, three and four complementary bases. We derive the explicit form of Alice and Bob mutual information and the information gained by each eavesdropper. In particular, we show that, in the presence of only one eavesdropper, the protocol involving four bases is safer than the other ones. However, for two eavesdroppers, the security is strongly dependent on the attack probabilities. The effect of a large number of eavesdroppers is also investigated.

[1] email: daoud@pks.mpg.de, m_daoud@hotmail.com

[2] email: ezahamid@fsr.ac.ma

1 Introduction

Inspired by Wiesner's ideas [1], Bennett and Brassard proposed in 1984 [2] a new approach to cryptography by developing a key distribution protocol , now known as BB84. Since then Quantum Key Distribution (QKD) constitutes one the most investigated concept in the quantum information theory. QKD provides a scheme to ensure a secure communication between two legitimate parties (usually called Alice and Bob) using quantum states that belong to non compatible bases. Quantum mechanics ensures that in quantum cryptographic protocols, the presence of an eavesdropper (often called Eve) in the communication channel can be detected through disturbances to the transmitted message. In the BB84 protocol [2], Alice and Bob randomly choose between two complementary bases and the information of each basis is encoded using the orthogonal states of a two dimensional quantum system. This protocol was extended in different ways. The first extension was proposed in [3]-[4] by adding an extra basis that is mutually unbiased compared to the other two in a two dimensional system. Cryptographic schemes, extending the BB84 model, based on d level quantum systems with M mutually unbiased bases were also developed. In this sense, a protocol using $d = 4$ states and $M = 2$ bases was studied in [5] and the case of $d = 3$ states and $M = 4$ bases was presented in [6]. This provided a way to formulate a generalized quantum key distribution involving quantum systems with arbitrary dimension d and using M mutually complementary bases [7]-[8].

The main task of quantum protocols, mentioned above as well as many others proposed in the literature, is traditionally to provide secure communications against only one eavesdropper. Recently, in [9], the authors discussed a scenario involving several eavesdroppers. This extends the BB84 protocol to take into account the effects induced by many potential eavesdroppers. In this paper, we replace, in the model introduced in [9], the two-level quantum systems (qubits) by optical biphoton qutrits. At this stage, it is important to note that three level optical systems constitute promising objects of modern quantum information and quantum cryptography. Indeed, the realization of optical qutrits with light has been approached using the polarization states of two indistinguishable photons -a biphoton [10] and their experimental manipulation was discussed in [11]. Also, quantum encoding based on polarization states of a biphoton was examined in [12].

To investigate quantum key distribution based on a three level optical system, we shall first develop, in the second section, a method to construct the phase states of a biphoton-system and we define the discrete operations generating four mutually unbiased bases from which Alice can choose to encode her message. A second facet of this work concerns the mutual information between Alice and Bob and the information intercepted by the eavesdroppers which employ the intercept-resend strategy. The explicit expressions of mutual informations as well as quantum errors are given, in the third section, in terms of the number N of eavesdroppers, the attack probabilities and the number M of complementary bases used by the sender to encode her message. In the last section, analysis of the security of the model in the particular cases of $N = 1$ and $N = 2$ are presented. We also discuss the case where the N eavesdroppers are collaborating (all intercept the sent message with identical probabilities).

Concluding remarks close this paper.

2 Qutrits, Phase states and mutually unbiased bases

2.1 Phase states

The biphoton qutrits are considered as superpositions of the three dimensional Fock space corresponding to the three possibilities of distributing two indistinguishable photons in two polarization modes horizontal (h) and vertical (v). The Fock space of purely polarized biphoton states is defined by

$$\mathcal{F} = \{|n_h, n_v\rangle \ , \ n_h + n_v = 2\} \tag{1}$$

where $|n_h, n_v\rangle$ is a Fock representation of n_h (n_v) horizontally (vertically) polarized photons. They are given by

$$|n_h, n_v\rangle = \frac{(a_h^+)^{n_h}}{\sqrt{n_h!}} \frac{(a_h^+)^{n_v}}{\sqrt{n_v!}} |00\rangle. \tag{2}$$

The vector $|0,0\rangle$ is the vacuum state and the objects a_h^+ and a_v^+ are the creation operators of photons with horizontal and vertical polarizations (with given equal frequencies and given identical propagation directions). The annihilation operators are defined as usual ($a_h^- = (a_h^+)^\dagger, a_v^- = (a_v^+)^\dagger$).

To introduce the phase states, we first define the unitary phase operator as in [13]

$$E = |2,0\rangle\langle 0,2| + |1,1\rangle\langle 2,0| + |0,2\rangle\langle 1,1|. \tag{3}$$

It is unitary. To find the phase states corresponding to this three level system, let us consider the eigenvalue equation

$$E|z\rangle = z|z\rangle, \qquad z \in \mathbf{C}. \tag{4}$$

By expanding the state $|z\rangle$ as a linear combination of the vector states of $\mathcal{F}$, it is easy to see that the eigenvalue z is given by

$$z = q^m = \exp\left(i\frac{2\pi m}{3}\right) \text{ with } m = 0, 1, 2, \tag{5}$$

and the normalized eigenstates of the operator E (the phase states) rewrite

$$|m\rangle = \frac{1}{\sqrt{3}}(|0,2\rangle + q^m|1,1\rangle + q^{2m}|2,0\rangle). \tag{6}$$

It follows that the states $|m\rangle$ satisfy

$$E|m\rangle = e^{i\theta_m}|m\rangle \qquad \theta_m = \frac{2\pi m}{3}, \tag{7}$$

which shows that they are indeed phase states and E is a unitary phase operator. The phase states are orthonormal ($\langle m'|m\rangle = \delta_{m',m}$). Then, Alice encodes her message in the computational basis generating the Fock space $\mathcal{F}$ or in the phase states basis $\{|m\rangle \ , \ m = 0, 1, 2\}$. It is important to note that Alice can use two others bases which can be generated from the phase states as shown in what follows.

2.2 Mutually unbiased bases

Recall that two d-dimensional bases are said to be unbiased if and only if the modulus of the inner product of any vector of one basis with any vector of the other one is equal to $1/\sqrt{d}$ [14]-[15]. The number M of mutually unbiased bases (MUBs) is such that $M \leq d+1$. The maximum number $M = d+1$ can be achieved when d is prime or a power of a prime [15]. Construction of MUBs associated with finite dimensional Hilbert space was considered via different methods as for instance ones based on discrete Fourier analysis over Galois fields and Galois rings, generalized Pauli matrices, angular momentum theory, etc (for a recent review and other methods of MUBs construction see [16]). Accordingly, the three level optical system we are considering, has four mutually unbiased bases. The first basis is the computational basis $B_3 := \{|2,0\rangle\ ,\ |1,1\rangle\ ,\ |0,2\rangle\}$ and the second one is generated by the phase states (6). Indeed, it is easy to check that the states (6) are unbiased to the computational basis . The two other remaining mutually unbiased bases can be generated as follows. We introduce the time evolution operator $U(t)$ defined by

$$U(t)|n_h, n_v\rangle = e^{ia_h^+ a_h^- a_v^- a_v^+ t}|n_h, n_v\rangle \tag{8}$$

in term of vertical and horizontal ladder operators. The operator $U(t)$ generates MUBs when acting on the phase states (6). Indeed, for the discrete values

$$t := t_p = \frac{p\pi}{3} \quad \text{with} \quad p = 0, 1, 2,$$

the states (6) transform as

$$U(t_p)|m\rangle := |p, m\rangle = \frac{1}{\sqrt{3}}(|0,2\rangle + q^{m+p}|1,1\rangle + q^{2m+p}|2,0\rangle). \tag{9}$$

Notice that for $p = 0$, the states $|0, m\rangle$ coincide with phase states (6) ($|0, m\rangle \equiv |m\rangle$). It is simply verified that the computational basis B_3 and the bases $B_p = \{|p, m\rangle\}$ ($p = 0, 1, 2$) are mutually unbiased. To close this section, it is important to note that the operator $U(t_p)$ is related to the quadratic discrete Fourier transform [16] and coincides with the so-called tritter [17] which is a generalization, in three dimensional case, of the 2×2 unitary operation characterizing a 50-50 beam splitter.

3 Eavesdropping strategy and mutual informations

As mentioned above, quantum key distribution in the presence of several eavesdroppers was developed in [9]. This scenario extends the BB84 protocol by investigating the effect of several eavesdropper intercept-resend attacks on the quantum error and mutual information between two legitimate parties. It was shown that the secured-unsecured transition depends strongly on the number of eavesdroppers and their probabilities of intercepting attacks. In this section, we investigate the effect of several eavesdroppers on the quantum cryptographic scheme using biphoton qutrits.

3.1 Eavesdropping strategy: the Model

Following the idea discussed by Bourenanne et al [7], we consider a protocol with M ($2 \leq M \leq 4$) mutually complementary bases and 3 orthogonal states in each base. We shall assume that this protocol is under attack by an arbitrary number N of eavesdroppers E_1 , E_2 , ..., E_N. Within this protocol, Alice first selects randomly one of the M bases in which she wants to encode her state and second decides which of the 3 optical states ($|0,2\rangle, |1,1\rangle$ or $|2,0\rangle$) to send. In other words, she sends to Bob random states in which the number of horizontally polarized photons is $0, 1, 2$ with equal probability of $1/3$. Bob measures each symbol sent by selecting at random between the M bases. Hence, the mutual information between Alice and Bob can be described by a joint probability $P(x_A, x_B)$. The random variables $x_A = 0, 1, 2$ and $x_B = 0, 1, 2$ represent the number of horizontally polarized photons prepared by the sender (Alice) and the measurement results obtained by the receiver (Bob). Between them a number N of eavesdropper E_i ($i = 1, ..., N$) are trying to intercept the sent message. Each eavesdropper E_i intercepts, with probability ω_i, the biphoton state emitted by the eavesdropper E_{i-1}. He or she measures its number of photons horizontally polarized by selecting at random, with probability $1/M$, between the M MUBs and resends it, in its measured state, to the eavesdropper E_{i+1}. At the place of the non measured biphoton polarization, with probability $1 - \omega_i$, the eavesdropper E_i sends randomly $0, 1, 2$, with equal probability $1/3$, to the eavesdropper E_{i+1}. In the same way, the eavesdropper E_{i+1} intercepts, with probability ω_{i+1}, the biphoton state emitted by the eavesdropper E_i, measures its number of photons polarized horizontally by selecting at random, with probability $1/M$, between the M MUBs, and resends it in its measured state to the eavesdropper E_{i+2} and so on. We note that the eavesdropper E_1 intercepts the state emitted by Alice and the eavesdropper E_N resends the biphoton to Bob.

Finally, in order to obtain a secret key, Alice and Bob use an authenticated public channel to estimate the error rate and the maximal quantity of information obtained by the eavesdroppers. However, if the error rate (called the error probability) is greater than a critical value (quantum error) Alice and Bob begin another protocol to establish another secret key until the error rate becomes smaller than the quantum error.

3.2 The mutual informations

To evaluate the mutual information between Alice and Bob and the amount of information gained by the eavesdroppers, the relevant information is the Shannon information of the sifted symbols, i.e., the symbols for which Alice and Bob have used the same bases. This information is measured in bits for simplicity.

Let us denote by $p(x)$ the prior probability for Alice to send the symbol x and $p(x|y)$ is the posteriori probability that is the conditional probability of the sending party having sent the symbol x and the receiver (Bob or Eves) measured the result y. The mutual information is (see for instance [7])

$$I_{AY} = \log_2 3 - H_{\text{apost}} \tag{10}$$

where Y stands for $B, E_1, E_2, \cdots, E_N$ and the quantity

$$H_{\text{apost}} = -\sum_y p(y) \sum_x p(x|y) \log_2 p(x|y) \tag{11}$$

is the aposteriori entropy. Using the symmetry properties of the protocol, it is easy to check that

$$I_{AY} = \log_2 3 + \sum_{n_h=0}^{2} p(n_h|0) \log_2 p(n_h|0). \tag{12}$$

The mutual information between Alice and Bob I_{AB} and between Alice and the m-th eavesdropper I_{AE_m} $(m = 1, 2, \cdots, N)$ are expressed in terms of the conditional probabilities which can be easily evaluated in terms of the attack probabilities using the eavesdropping strategy discussed above.

Using the expression (12), we can hence obtain the mutual information between Alice and Bob

$$I_{AB} = \log_2 3 + P_{AB}(0|0) \log_2(P_{AB}(0|0)) + [1 - P_{AB}(0|0)] \log_2 \left[\frac{1 - P_{AB}(0|0)}{2}\right], \tag{13}$$

in term of the conditional probability $P_{AB}(0|0)$. Based on the assumptions defining the eavesdropping strategy, one can show that this probability takes the following form

$$P_{AB}(0|0) = \sum_{k=0}^{N} a_k(N) \Omega_k(N) \tag{14}$$

where the coefficients $a_k(N)$ are given by

$$a_k(N) = \frac{1}{M^{N-k}} \left[1 + \frac{M-1}{3} \sum_{i=0}^{N-k-1} M^i\right], \tag{15}$$

and the quantities $\Omega_k(N)$ are expressed in term of eavesdroppers attack probabilities as

$$\Omega_k(N) = \omega_1 \omega_2 \cdots \omega_N \sum_{i_1 < i_2 < \cdots < i_k} \left[\frac{1 - \omega_{i_1}}{\omega_{i_1}} \frac{1 - \omega_{i_2}}{\omega_{i_2}} \cdots \frac{1 - \omega_{i_k}}{\omega_{i_k}}\right] \tag{16}$$

for $k \neq 0$ and the indices i_j take the values $1, \cdots, N$. For $k = 0$,

$$\Omega_0(N) = \omega_1 \omega_2 \cdots \omega_N. \tag{17}$$

Similarly, using equation (12), it is simple to show that the direct reconciliation information between Alice and the m-th eavesdropper is given by

$$I_{AE_m} = \log_2 3 + P_{AE_m}(0|0) \log_2(P_{AE_m}(0|0)) + [1 - P_{AE_m}(0|0)] \log_2 \left[\frac{1 - P_{AE_m}(0|0)}{2}\right], \tag{18}$$

where

$$P_{AE_m}(0|0) = \frac{1 - \omega_m}{3} + \sum_{k=0}^{m-1} a_k(m) \Omega_k(m). \tag{19}$$

The lost information between the honest parties Alice and Bob corresponds to the maximum information intercepted by the entire eavesdroppers. This is given by

$$I_{AE} = \text{Max}\Big(I_{AE_1}, I_{AE_2}, \cdots, I_{AE_{N-1}}, I_{AE_N}\Big). \tag{20}$$

The error rate or the error probability $\mathrm{P_{err}}$ is defined by

$$\mathrm{P_{err}} = \sum_{x_A, x_B} \left| P_{AB}(x_A/x_B)\big|_{\omega_i=0} - P_{AB}(x_A/x_B)\big|_{\omega_i\neq 0} \right|. \tag{21}$$

The quantum error $\mathrm{Q_{err}}$ is the value of the error probability $\mathrm{P_{err}}$ for which $I_{AB} = I_{AE}$. It follows that for $\mathrm{P_{err}} < \mathrm{Q_{err}}$ we have $I_{AE} < I_{AB}$, while for $\mathrm{P_{err}} > \mathrm{Q_{err}}$ we have $I_{AE} > I_{AB}$.

4 Results and discussion

As illustration of the analysis developed in the previous section, we investigate in what follows the security of the protocol based on optical qutrit states in the presence of several eavesdroppers, in some particular cases.

4.1 One eavesdropper and mutual informations

In the situation where only one eavesdropper is trying to intercept the message sent by Alice ($\omega_1 = \omega$), the equation (14) gives

$$P_{AB}(0|0) = \frac{1}{M}\left(1 + \frac{M-1}{3}\right)\omega + (1-\omega). \tag{22}$$

Similarly from equation (19), one obtains

$$P_{AE}(0|0) = \frac{1-\omega}{3} + \frac{1}{M}\left(1 + \frac{M-1}{3}\right)\omega. \tag{23}$$

Reporting the conditional probabilities (22) and (23) in the equations (13) and (18), respectively, one has the mutual information I_{AB} and I_{AE}. The behavior of I_{AB} and I_{AE} as function of the attack probability ω are plotted in the figure 1.a.

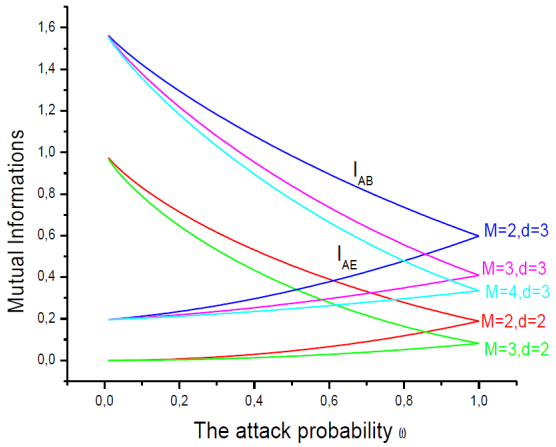

FIG. 1.a: Mutual information I_{AB} and I_{AE} as a function of the attack probability ω for qubits and qutrits.

As expected, the mutual information between Alice and Bob and the amount of information intercepted by Eve coincide for $\omega = 1$. In figure 1.a, we also plotted the mutual information I_{AB} and I_{AE}

when the sender uses a two dimensional system with two or three mutually unbiased bases to encode her message. The explicit expressions of I_{AB} and I_{AE} are given in the appendix. They are computed similarly to ones derived in the previous section for a three level system. This helps us to compare the amount of mutual information when Alice uses qubits or qutrits as it shown in the figure 1.a. Note that the obtained mutual information for $d = 2$ and $M = 2$ are in agreement with the results derived in [9].

To examine the security of the protocol, we studied the mutual information between the legitimate parties Alice and Bob I_{AB} and lost information I_{AE} as function of the error probability (Figure 1.b).

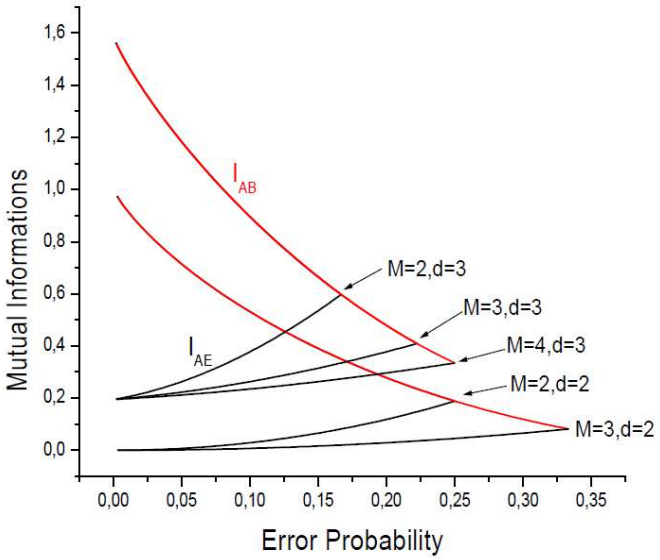

FIG. 1.b: Mutual information I_{AB} and I_{AE} as a function of quantum error Q_{err} for qubits and qutrits.

In this figure, we give the behavior of I_{AB} and I_{AE} for $d = 3$ when Alice chooses to encode her message using two, three or four complementary bases in the presence of only one eavesdropper. We evaluate the quantum error for each case. The results are summarized in table 1. In figure 1.b, we also present the information I_{AB} and I_{AE} for qubits ($d = 2$) as a function of error probability. This is useful in order to compare our results with ones obtained within the BB84 protocol and the protocol involving qubits with six states ($M = 3$) (see [3] and [4]). In this particular case, we evaluate the quantum error for $M = 2$ and $M = 3$. The results are given in table 1. It is clear from the figure as well as the table 1 that the protocol using ($d = 2$) with ($M = 3$) appears to provide better security. It is also important to stress that the quantum error in the case $d = 3$ and $M = 4$ provides the same quantum error as in the BB84 protocol. This shows that in a protocol involving three level systems, Alice should use four mutually unbiased bases to ensure the security of her sent information. It must be noticed that for d fixed, the quantum error increases with increasing values of the number of mutually unbiased bases M. In this respect, Alice must encode her message using all the available mutually unbiased bases to minimize the eavesdropping effects.

M	2	3	4
$d=3$	0.167	0.222	0.250
$d=2$	0.25	0.335	

Table 1: Quantum error for two and three level systems.

4.2 Two eavesdroppers and mutual information

Now, we consider the situation where two eavesdroppers E_1 and E_2 attack with probabilities ω_1 and ω_2, respectively. In this case, the equation (14) takes the simple form

$$P_{AB}(0|0)=\frac{1}{M^2}\left(1+\frac{M^2-1}{3}\right)\omega_1\omega_2+\frac{1}{M}\left(1+\frac{M-1}{3}\right)\Big(\omega_1(1-\omega_2)+(1-\omega_1)\omega_2\Big)+(1-\omega_1)(1-\omega_2). \quad (24)$$

Similarly, from equations (19), one has

$$P_{AE_1}(0|0)=\frac{1-\omega_1}{3}+\frac{1}{M^2}\left(1+\frac{M^2-1}{3}\right)\omega_1\omega_2, \quad (25)$$

and

$$P_{AE_2}(0|0)=\frac{1-\omega_2}{3}+\frac{1}{M^2}\left(1+\frac{M^2-1}{3}\right)\omega_1\omega_2+\frac{1}{M}\left(1+\frac{M-1}{3}\right)\Big((1-\omega_1)\omega_2\Big). \quad (26)$$

Substituting (24) into (13), one gets the mutual information I_{AB} between Alice and Bob. The conditional probabilities (25) and (26) together with the equations (18) and (20) give the lost information to the eavesdropper, I_{AE}. The figure 2.a represents the mutual information I_{AB} and I_{AE} (for $d=3$ and $M=2$) as function of the attack probability ω_1 of the first eavesdropper for different values of the attack probability of the second eavesdropper.

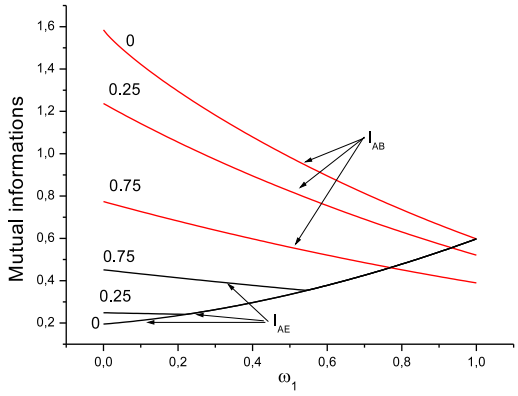

FIG. 2.a: Mutual information I_{AB} and I_{AE} as a function of the attack probability ω_1 for different values of ω_2.

It clear that I_{AB} and I_{AE} depend strongly on the values ω_1 and ω_2 and the mutual information between the legitimate parties decreases as ω_1 and ω_2 increase. The limiting case $\omega_2=0$ corresponds

to the protocol involving only one eavesdropper. In this case, the amount of information gained by the eavesdropper increases to intercept the information exchanged by Alice and Bob at $\omega_1 = 1$. But, when $\omega_2 \neq 0$, the information intercepted by the eavesdroppers intersect I_{AB} for $\omega_{1\text{tr}} \simeq 0.92$ when $\omega_2 = 0.25$ and for $\omega_{1\text{tr}} \simeq 0.76$ when $\omega_2 = 0.75$. Hence, for $\omega_1 > \omega_{1\text{tr}}$, the amount of information lost becomes greater that one exchanged between Alice and Bob and occurs at the transition from the secured to unsecured phase.

To understand the security of quantum key distribution based on qutrits in presence of two eavesdroppers, we studied the transition between the secured and unsecured phases. We note that in the secured phase, the error probability is smaller than the quantum error, while in the no secured phase the error probability is greater than the quantum error. At the transition line, the error probability coincides with the quantum error. Phase diagram, in the space parameter (ω_1, ω_2), is presented in the figure 2.b. This shows the transition line between secured and no secured phases. In contrast to the case of the protocol with one eavesdropper for which the secured-unsecured transition occurs at an intercept probability $\omega_1 = 1$, the region of secured phase depends on both intercept probability rates ω_1 and ω_2. We consider the situations where Alice uses two, three and four mutually bases.

From figure 2.b, it is easily seen that for $0 < \omega_1 < 0.55$, the line transition between the secured and unsecured phase is ω_2-independent. It is also independent of the number of mutually independent bases M used by Alice. This changes drastically when the probability attack of the eavesdropper E_1 becomes grater than 0.55. In this case, the transition depends strongly on the values of attacks probability of the second eavesdropper as well as the mutually unbiased bases M. The transition probability, at the transition line, increases with decreasing ω_2

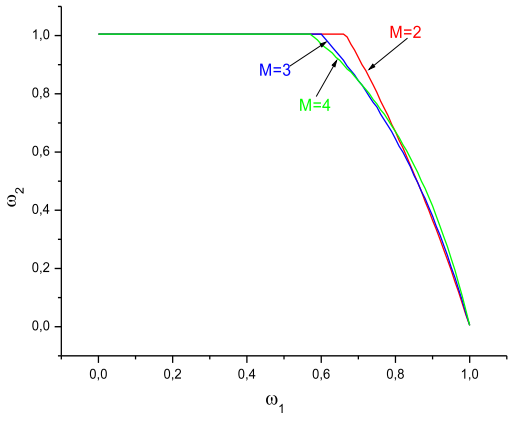

FIG. 2.b: The (ω_1, ω_2) phase diagram for qutrits.

To clarify the behavior of the transition from the secured to unsecured phase for $0.55 \leq \omega_1 \leq 1$, we give the figure 2.c where the line transition is represented for $M = 2, M = 3$ and $M = 4$. From this figure, one can see that for $0.55 < \omega_1 < 0.67$, the protocol involving $M = 4$ complementary bases gives less security than the two others using two and three bases. This situation becomes different in the region $0.67 < \omega_1 < 0.86$; Indeed, in this case the model with $M = 3$ provides less security. Finally,

for $\omega_1 > 0.86$, when Alice uses only two complementary bases, the area of secured phase is reduced in comparison to ones corresponding to the secured phases obtained with $M = 3$ and $M = 4$.

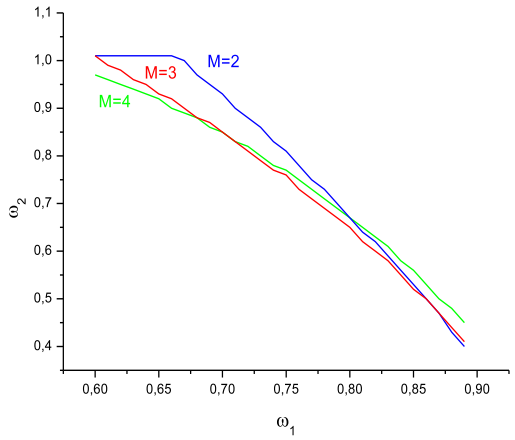

FIG. 2.c: The (ω_1, ω_2) phase diagram for $0.55 \leq \omega_1 \leq 1$.

4.3 Many eavesdroppers

Now, we shall discuss the situation where the eavesdroppers communicate between them and try to intercept the same state with identical probability $\omega_i = \omega$ for $i = 1, 2, \cdots, N$. In this case, the equation (14) takes the simple form

$$P_{AB}(0/0) = \frac{1}{3} + \frac{2}{3}\left[1 + \frac{\omega}{M}(1 - M)\right]^N, \tag{27}$$

and the equation (19) gives

$$P_{AE_m}(0/0) = \frac{1}{3} + \frac{2}{3}\frac{\omega}{M}\left[1 + \frac{\omega}{M}(1 - M)\right]^{m-1}. \tag{28}$$

The (ω, N)-phase diagram (Figure 3.a) shows the secured-unsecured transition when the N eavesdroppers are collaborating and attack with the same probability ω.

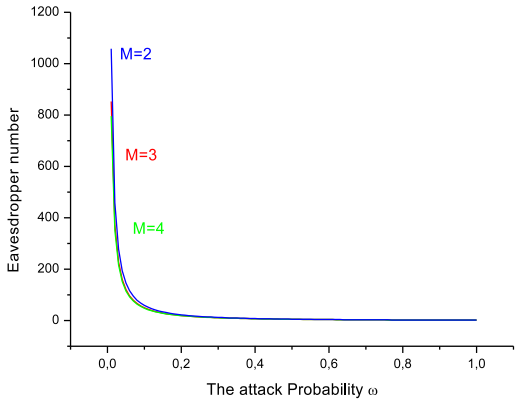

FIG. 3a: The (ω, N)-phase diagram.

The security of the protocol decreases when N increases. Moreover, in the region $(0.1 \leq \omega \leq 1, 0 \leq N \leq 50)$, the security of the protocol is completely independent of the number M of mutually unbiased bases used by the sender. However, for $N \geq 50$ and $0 \leq \omega \leq 0.1$ (see figure 3.b), more security is provided by the protocol involving two complementary bases (i.e., $M = 2$).

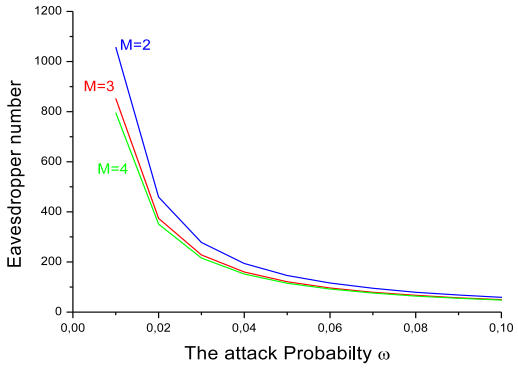

FIG. 3b: The (ω, N)-phase diagram.

5 Concluding remarks

We have considered quantum cryptographic scheme where bi-photon qutrits are used to encode the information. Using the Pegg-Barnett phase operator, we defined the four mutually unbiased bases of this three level system. This is mainly based on the phase states approach. To compare the qutrits based cryptographic protocols with their qubits based counterpart, we also investigated the bi-dimensional quantum systems when the sender uses two or three bases in the presence of many eavesdroppers. In the situation where only one eavesdropper is involved, for a two level quantum system, the protocol based on three complementary bases is safer than the BB84 one which uses two bases only. We have shown that when Alice and Bob exchange information using qutrits, the safer scenario corresponds to one using four mutually unbiased bases. It follows that for $d = 2$ as well as $d = 3$, to ensure the security of the sent information, Alice should encode her message using all the available complementary bases of the Hilbert space of the quantum system under consideration. It is important to note that the quantum error for the scheme involving four mutually unbiased bases coincides with the one obtained in BB84 protocol. It seems that for higher dimensional quantum systems, the maximal security is reached when the sender uses all available complementary bases. These results change drastically when more than one eavesdropper attempt to intercept the information exchanged between the legitimate parties. Indeed, the secured-unsecured transition for qutrits is strongly dependent on the attack probabilities ω_1 and ω_2. In this case many scenarios are possible and there is a concurrence between the protocols involving two, three or four mutually unbiased bases. Finally, we have shown that the number of the eavesdroppers reduces the area of secured phase and the protocol becomes less secure. In particular, we examined the case where a large number of collaborating eavesdroppers are trying to intercept the information with equal probability ω. This

shows clearly that the number of eavesdroppers is very important in dealing with the security of any quantum cryptographic key distribution protocol .

Acknowledgments

MD would like to thank the hospitality and kindness extended to him by the Max Planck Institute for Physics of Complex Systems (Dresden, Germany) where this work was done.

Appendix

It is well known that for a two dimensional quantum system, there is three maximally unbiased bases from which Alice can choose $M = 2$ or $M = 3$ bases to encode her message. Similarly to the qutrits case discussed above and using the same assumptions, the mutual information between Alice and Bob, in presence of one eavesdropper only, can be found as

$$I_{AB} = 1 + P_{AB}(0|0)\log_2(P_{AB}(0|0)) + [1 - P_{AB}(0|0)]\log_2\left[\frac{1 - P_{AB}(0|0)}{2}\right],$$

where

$$P_{AB}(0|0) = 1 - \frac{\omega}{2}\frac{M-1}{M}.$$

The intercepted information by the eavesdropper is

$$I_{AE}(0|0) = 1 + P_{AE}(0|0)\log_2(P_{AE}(0|0)) + [1 - P_{AE}(0|0)]\log_2\left[\frac{1 - P_{AE}(0|0)}{2}\right],$$

where

$$P_{AE} = \frac{1}{2}\left(1 + \frac{\omega}{M}\right).$$

For two eavesdroppers E_1 and E_2, trying to intercept the sent information with probabilities ω_1 and ω_2, the conditional probabilities are given by

$$P_{AB}(0|0) = 1 - \frac{M-1}{2M}(\omega_1 + \omega_2) + \frac{(M-1)^2}{2M^2}\omega_1\omega_2,$$

$$P_{AE_1}(0|0) = \frac{1}{2}\left[1 - \omega_1(1 - \omega_2) + \frac{\omega_1\omega_2}{M^2}\right],$$

and

$$P_{AE_2}(0|0) = \frac{1}{2}\left[1 + \frac{\omega_2}{M} - \frac{M-1}{M^2}\omega_1\omega_2\right]$$

from which one can evaluate the mutual informations I_{AB}, I_{AE_1} and I_{AE_2}.

References

[1] S. Wiesner, *Conjugate coding* , Sigact News,**15**, 78 (1983).

[2] C.H. Bennett and G. Brassard in *Proceeding of the IEEE International Conference on Computer, Systems and Signal Processing*, Bangalore, India (IEEE Press, New York,1984).

[3] D. Bruß, Phys. Rev. Lett. **81** 3018 (1998).

[4] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59** 4238 (1999).

[5] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61** 062308 (2000).

[6] H. Bechmann-Pasquinucci and A. Peres, `quant-ph/0001083`.

[7] M. Bourennane, A. Karlsson and G. Björk, Phys. Rev. A **64** 012306 (2001).

[8] N. Cerf, M. Bourennane, A. Karlsson and N. Gisin, Phys. Rev. Lett **88** 127902 (2002).

[9] H. Ez-zahraouy and A. Benyoussef, Int. J. Mod. Phys. **B 23** 4755 (2009).

[10] Yu. Bogdanov, M. Chekhova, S. Kulik, G. Maslennikov, C.H. Oh, M.K. Tey and A. Zhukov, Phys. Rev. Lett. **93** 230503 (2004).

[11] B.P. Lanyon, T.J. Weinhold, N.K. Langford, J.L. O'Brien, K.J. Resch, A. Gilchrist and A.G. White, Phys. Rev. Lett. **100** 060504 (2008).

[12] I. Bregman, D. Aharonov, M. Ben-Or and H.S. Eisenberg, Phys. Rev. A **77** 050301(R) (2008).

[13] D.T. Pegg and S.M. Barnett, Phys. Rev. A **39** 1665 (1989).

[14] I.D. Ivanović, J. Phys. A: Math. Gen. **14** 3241 (1981).

[15] W.K. Wootters and B.D. Fields, Ann. Phys. (N Y) **191** 363 (1989).

[16] M.R. Kibler, J. Phys. A: Math. Theor. **41** 375302 (2008); J. Phys. A: Math. Theor. **42** 353001 (2009).

[17] M. Z-dotukowski, A. Zeilinger and M.A. Horne, Phys. Rev. **A 55** 2579 (1997).